

The Writhe of Permutations and Random Framed Knots

Chaim Even-Zohar*

January 6, 2016

Abstract

We introduce and study the *writhe* of a permutation, a circular variant of the well-known inversion number. This simple permutation statistics has several interpretations, which lead to some interesting properties. For a permutation sampled uniformly at random, we study the asymptotics of the writhe, and obtain a non-Gaussian limit distribution.

This work is motivated by the study of random knots. A model for random framed knots is described, which refines the Petaluma model, studied in [11]. The distribution of the framing in this model is equivalent to the writhe of random permutations.

1 Introduction

As usual we denote $\mathbb{Z}_{2n+1} = \mathbb{Z}/(2n+1)\mathbb{Z}$. Let $f : \mathbb{Z}_{2n+1} \rightarrow \mathbb{R}$ be one-to-one. We define the *writhe* of f as follows.

$$w(f) = \sum_{i=0}^{2n} \sum_{j=1}^n \text{sign}(f(i+j) - f(i))$$

where $\text{sign}(x) = +1$ if $x > 0$ and -1 if $x < 0$.

Let's examine this definition. We sum over all pairs $x, y \in \mathbb{Z}_{2n+1}$ and compare the values of $f(x)$ and $f(y)$. Viewing \mathbb{Z}_{2n+1} as a set of points evenly distributed on the unit circle, say clockwise, we may “connect” x and y through the shorter arc. Then we add one if f is clockwise increasing on the pair (x, y) , and subtract one if it's decreasing. Intuitively, the writhe measures to what extent a function on the discrete circle is clockwise increasing or decreasing.

Note that in this definition only the relative ordering of the values in $\text{Image}(f)$ matters, and not the actual values. Hence it is natural to study the writhe for all one-to-one functions $f : \{0, \dots, 2n\} \rightarrow \{0, \dots, 2n\}$. The main subject of this paper is the distribution of the writhe for uniformly sampled permutations in S_{2n+1} .

Both the term writhe and our interest in the subject originated in knot theory. In [11], we study a model for random knots, in which a permutation $\pi \in S_{2n+1}$ defines a knot, through a petal diagram, from [1]. In Section 2, we refine this random model to deal with *framed* knots, and observe that the knot's *framing* is equal to the writhe of π .

However, writhe seems to carry an independent interest as a combinatorial concept. Note its similarity with the inversion number of a permutation, $\text{inv}(\pi) = \#\{(x, y) : x < y, \pi(x) > \pi(y)\}$, which plays a central role in enumerative combinatorics as well as in sorting and ranking algorithms. In a sense, $\text{inv}(\pi)$ measures the distance of π from the identity. For example, the Mallows model is a well-known non-uniform distribution of permutations, in which the probability of a permutation π is proportional with $q^{\text{inv}(\pi)}$, for some $q > 0$ [20, 8, 3].

In a similar spirit, the writhe quantifies how shuffled a given permutation $\pi : \mathbb{Z}_{2n+1} \rightarrow \mathbb{Z}_{2n+1}$ is. It is easily verified that the writhe is invariant under rotations from both sides. Namely, $w(\pi) = w(\pi \circ \rho) = w(\rho \circ \pi)$ where $\rho(x) = x + 1 \pmod{(2n+1)}$. Indeed the appropriate geometry for the writhe is that of the circle \mathbb{Z}_{2n+1} , whereas $\text{inv}(\pi)$ suits a linear order.

*Department of Mathematics, Hebrew University, Jerusalem 91904, Israel.
e-mail: chaim.evenzohar@mail.huji.ac.il .

In Section 3 we discuss the relation of the writhe to other combinatorial notions, such as the *alternating inversion number* [5], and *circular bubble sort* [17, 24]. We also fit the writhe into the context of nonparametric statistics for *circular rank correlation* [13, 14]. An algorithm to compute the writhe in time $O(n \log n)$ is described, inspired by notions from knot theory.

The main result of this work is the distribution of the writhe of a uniformly chosen random permutation from S_{2n+1} . Although the writhe takes values in $[-n^2, n^2]$, we show that typically it is linear in n , in a strong sense which we turn to describe.

We think of the writhe as a random variable and consider its moments $E[w^k]$. All odd moments vanish, since reversing π flips the writhe's sign. We determine the asymptotics of the k th moment for even k .

Theorem 1. *Let $\pi_{2n+1} \in S_{2n+1}$ be drawn uniformly at random. Then*

$$E \left[\frac{w(\pi_{2n+1})^k}{n^k} \right] \xrightarrow{n \rightarrow \infty} \sum_{\sigma \in S_k} \prod_{\gamma \in \text{cycles}(\sigma)} \lambda_{|\gamma|},$$

where for even m

$$\lambda_m = \frac{8^m (2^m - 1) B_m^2}{2(m!)^2},$$

and $\lambda_m = 0$ for odd m . B_m stands for the m th Bernoulli number.

These limits are proved in Section 4, where we also give a formula for lower order terms. Our methods extend previous work on invariants of random knots [11], and work by Mingo and Nica [22].

Define the *normalized writhe* of a random permutation $\pi \in S_{2n+1}$, as $W_{2n+1} = w(\pi)/n$. Theorem 1 yields the limits of the moments of the normalized writhe, e.g.

$$E[W_{2n+1}^2] \xrightarrow{n \rightarrow \infty} \frac{2}{3} \qquad E[W_{2n+1}^4] \xrightarrow{n \rightarrow \infty} \frac{76}{45}$$

We use the method of moments to derive from Theorem 1 convergence in distribution of the normalized writhe.

Corollary 2. *There exists a continuous distribution W on \mathbb{R} such that*

$$W_{2n+1} \xrightarrow[n \rightarrow \infty]{D} W,$$

and W is defined by the moment generating function

$$\mathcal{M}(z) = E[e^{Wz}] = \exp \left(\sum_{m=0}^{\infty} \frac{\lambda_m}{m} z^m \right).$$

where λ_m is as in Theorem 1.

See Figure 1 for the probability density function of W . In Section 5 we prove Corollary 2, and investigate some properties of W . It turns out that the tails of the distribution of the normalized writhe decay exponentially, at the asymptotic rate given below.

$$\lim_{t \rightarrow \infty} \frac{\log P[|W| > t]}{t} = -\frac{\pi^2}{4} \approx -2.47.$$

We present some alternative characterizations of the limit distribution. The infinite series in Corollary 2 may be traded for a definite complex integral, which is stated in Section 5 as well. We also represent W as an infinite sum. Let A be a random variable with density $f_A(x) = 1/\pi \cosh x$, and let $A_n \sim A$ iid. Then the infinite sum $\sum_{n=1}^{\infty} \frac{1}{n} A_n$ converges almost surely to a random variable having the same distribution as W . Refinements of this series yield further representations of W , using Laplace random variables, or products of Gaussians.

We note that none of these properties provides an efficient way to sample from W or compute its percentiles. It is still desirable to find a closed form formula for that purpose.

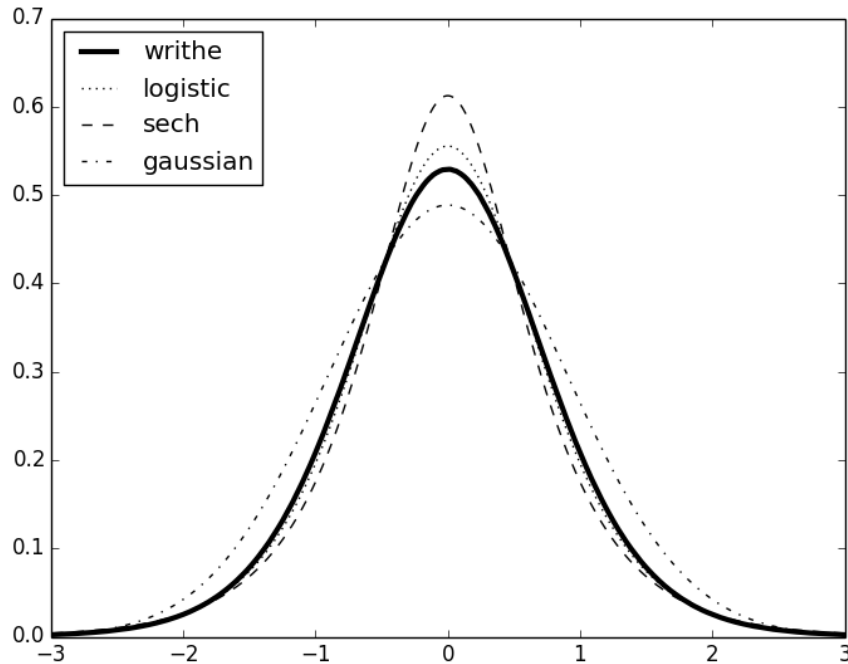


Figure 1: The writhe distribution with friends. The probability density function of W , the limit distribution of the normalized writhe is given by the solid line. The Gaussian, Logistic, and Sech distributions with variance $2/3$ are given for comparison.

Acknowledgment

I wish to thank Joel Hass, Nati Linial, and Tahl Nowik for many hours of insightful discussions on random knots in general, and on the subject of this work. I also wish to thank Yuval Peres for a helpful discussion. This project was supported by BSF grant 2012188.

2 Random Framed Knots

We begin with describing the relation to random framed knots. More background on framed knots can be found, e.g., in [6], and for further information on the random model, see [1, 11]. Readers interested mainly in the combinatorial aspect may skip this section.

2.1 Framed Knots

A *knot* is a simple closed curve in 3 dimensions, or more precisely, a smooth embedding $S^1 \hookrightarrow \mathbb{R}^3$ up to the following equivalence. Two such curves represent the same knot iff one can be deformed into the other through an isotopy of the ambient space.

A knot can be represented by a *knot diagram*, which is its projection to the plane, with a finite number of double points, called *crossings*, marked to distinguish the over-strand from the under-strand. See Figure 2A for a diagram of the *figure-eight* knot.

A *framed knot* is equipped with a normal vector, defined continuously at each point of the curve. By pushing the curve a bit along the framing vectors, one obtains an embedding of an orientable closed ribbon $[0, \varepsilon] \times S^1$, as illustrated in Figure 2B.

A natural way to choose a framing given a knot diagram, is parallel to the plane of the projection. This choice is called the *blackboard framing*, since it can be obtained by drawing two parallel copies

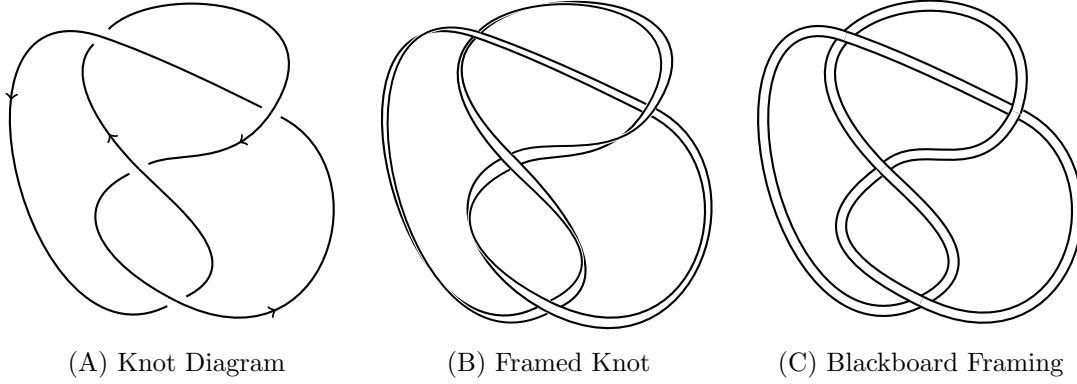


Figure 2: The figure eight knot, with two framings.

of the knot diagram, as in Figure 2C.

2.2 Writhe and Framing

There are two types of crossing points in knot diagrams: positive \nearrow , and negative \searrow . We first define the *writhe of a knot diagram* D , as a signed sum over crossings in a the diagram. Namely,

$$w(D) = \#\nearrow - \#\searrow$$

where the count is over all crossings in D . For example, the writhe of the diagram in Figure 2A is 0, as the two points in the lower part of the diagram are positive, and the other two are negative. The writhe cannot be pulled back to an isotopy invariant of knots, since it is not preserved under the following local change of diagrams, $\smile \Leftrightarrow \frown$, known as the Reidemeister move of type I. A well-known use of the writhe appears in the definition of the Jones Polynomial through the Kauffman Brackets [18].

A *link* is a collection of knots, or more precisely, a smooth embedding of a disjoint union of copies of S^1 into \mathbb{R}^3 , as usual considered up to isotopies. Let L be a two-component link, and let D be an arbitrary link diagram of L . The *linking number* is a well-known link invariant, firstly defined by Gauss [15]. Here we use the definition

$$lk(L) = \frac{1}{2} (\#\nearrow - \#\searrow)$$

where the count is only over crossings in D that involve one strand from each component. One can show that the linking number doesn't depend on the choice of the diagram D . Hence it is well-defined as a link invariant. For example, $lk(\bigcirc \bigcirc) = 1$, as both crossings are positive and involve the two components.

The *framing number* of a framed knot, also known as its *self-linking*, is defined as the linking number of the knot, with the parallel curve obtained by small pushing in the direction of the framing vector, cf. Figure 2B. The framing number is 0 exactly when the ribbon described above can be extended to an embedded oriented surface whose boundary is the original knot. Since it is preserved under continuous deformations, the framing number is an invariant of framed knots. In fact, a framed knot is characterized by its framing number and the underlying knot type.

By the above definition, the framing number of the blackboard framing of a given knot diagram is equal to the writhe of that diagram, and hence can be computed as a sum of crossing signs. Indeed, each crossing in the knot diagram corresponds to four crossings in the link obtained from its blackboard framing. Two of these crossings involve the different components, the sign of both is equal to that of the original crossing. This is balanced by the coefficient $\frac{1}{2}$ in the formula for the linking number.

The reader should be warned, however, that these two notions do not necessarily coincide for projections of framed knots that are not given by blackboard framing. For example, while both in Figures 2B and 2C the writhe of the diagram is 0, the framing numbers of the knots are different,

specifically 1 and 0 respectively. In general, the difference between the framing number of a framed knot and the writhe of its projection counts, in some appropriate sense, how many times the framing vector twists around the projected knot [2].

We mention two basic properties of the writhe that follow easily from the definition. Changing the orientation of the diagram preserves its writhe, while passing to a mirror image or flipping all crossings negates it.

Remarks. See [6] or [11] for definitions and more details on the following notions.

1. A *Gauss diagram formula* for the writhe is given by

$$w(D) = \left\langle \begin{array}{c} \text{diagram with two crossings} \\ \text{diagram with one crossing} \\ \text{diagram with one crossing} \\ \text{diagram with one crossing} \end{array}, D \right\rangle = \left\langle \begin{array}{c} \text{diagram with two crossings} \\ \text{diagram with one crossing} \\ \text{diagram with one crossing} \\ \text{diagram with one crossing} \end{array}, D \right\rangle$$

2. The framing number is a *first order finite type invariant* of framed knots.

2.3 The Random Model

A *petal diagram* is a closed planar curve, comprised of $2n + 1$ straight segments crossing at a single point, and arcs connecting consecutive pairs of segment tips. See Figure 3A for a petal diagram with 7 petals. Adams et al. showed that this representation is universal, i.e., every knot can be positioned so that it has a petal projection [1].

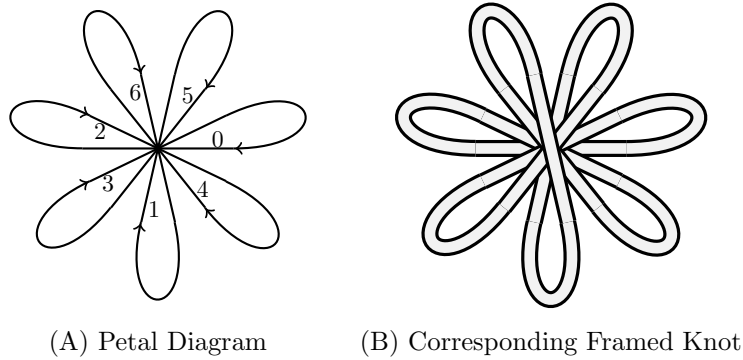


Figure 3: A diagram with 7 petals, and its blackboard framing.

Consider a petal diagram with $2n + 1$ petals. The only variable is the relative ordering of the heights of the arcs in the original knot, as they pass straightly above the center point. This ordering is encoded by a permutation $\sigma \in S_{2n+1}$, that assigns a height to each arc, as marked in Figure 3A. In the *Petaluma* model, we generate a random knot, simply by picking σ uniformly at random [11].

There is a natural extension of this random model to framed knots. We assign the blackboard framing to a petal diagram, with random $\sigma \in S_{2n+1}$ as in the Petaluma model, to obtain a random framed knot. This model is universal for framed knots – see Proposition 3 below. See also Figure 3B for an illustration of a random framed knot. In the rest of this section, we will draw knot diagrams without the double lines that indicate the use of the blackboard framing.

What is the writhe of a petal knot diagram? Note that petal diagrams are not a special case of regular knot diagrams, because here the center point has more than two pre-images. However, the arcs above the center can be slightly perturbed without changing the knot type so as to obtain a decent knot diagram with $\binom{2n+1}{2}$ crossings. These crossings correspond to all pairs of the $2n + 1$ arcs, and the writhe is the sum of their signs.

These signs depend on the arcs' directions and heights. Without loss of generality, number the arcs clockwise according to their directions in the plane of the diagram. These directions are equally placed with angles of $2\pi/(2n + 1)$ in between. Given a pair of arcs i, j , such that $(j - i) \bmod (2n + 1) \in \{1, \dots, n\}$, the sign of their crossing is positive if $\pi(i) < \pi(j)$ and negative otherwise. Therefore, the writhe of the petal diagram defined by π coincides with the writhe of the permutation π , as defined in the introduction to this paper.

2.4 Variations

We proceed with a few simple manipulations to petal diagrams, that will come useful later.

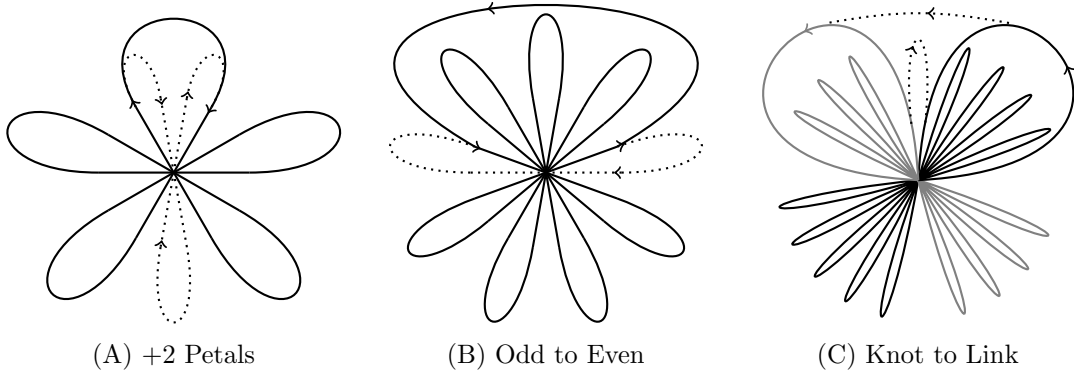


Figure 4: Three manipulations of petal diagrams.

(A) We add two petals to a given petal diagram, as in Figure 4A. If the two new arcs are assigned with two consecutive heights, then the unframed knot type is unchanged. Indeed, one can pull the whole supplement back to the original knot. Moreover, since the new arcs have adjacent heights and opposite directions, their crossings with any third arc have opposite signs, with no contribution to the writhe. The only change to the writhe comes from the crossing between the two new arcs, which is ± 1 , depending on the choice of heights.

By iterating this move, we can set the writhe at will. As a framed knot is determined by its unframed knot type and framing number, we conclude that the Petaluma model is universal for framed knot, in the following sense.

Proposition 3. *For every framed knot K there exists a number $N \in \mathbb{N}$, such that for every $n \in \{N, N+2, N+4, \dots\}$, K can be realized by a petal diagram with $2n+1$ petals.*

(B) One can take the highest arc in a $(2n+1)$ -petal diagram, and continuously move it outside, as illustrated in Figure 4B for $n=4$. This operation preserves both the knot type and the writhe. Indeed, since the highest arc is moved away, exactly n of the $2n$ eliminated crossings are positive, and n are negative. Hence the new, $2n$ -petal diagram in Figure 4B yields the same framed knot. In conclusion, a random permutation $\pi \in S_{2n}$ yields a random framed knot, equivalent in distribution to the one obtained from $(2n+1)$ -petal diagrams.

(C) Two petal diagrams, with $2l$ and $2r$ petals, can be superpositioned to create a 2-component link diagram with $2(l+r)$ petals and a single multi-crossing point. See Figure 4C for an example with 10 and 8 petals, colored black and gray respectively. A permutation $\pi \in S_{2(l+r)}$ can determine the heights of all arcs and yield a link. This representation is universal for links [1]. Similar to framed knots, by taking π uniformly at random and using the blackboard framing, we obtain a random *framed link*. This model extends further to more than two components.

By reconnecting the two large petals of a link diagram, as do the dotted arcs in Figure 4C, one obtains a petal diagram of a knot, without changing any crossing or introducing new ones. Comparing the sum of crossing signs yields the relation

$$w(K) = w(K_L) + w(K_R) + 2 \cdot lk(K_L, K_R)$$

where K_L and K_R are the two components in the link diagram, and K is the combined knot diagram.

3 Properties and Connections

In the following sections, we study several features of the writhe, and how they are reflected by different viewpoints, pointing at the relation of the writhe to previously studied notions.

3.1 Alternating Inversion Numbers

We give an equivalent expression for the writhe of a permutation. First, consider the following three statistics of a permutation $\sigma \in S_N$.

$$\begin{aligned}\iota(\sigma) &= \sum_{0 \leq y < x < N} \text{sign}(\sigma(x) - \sigma(y)) \\ \hat{\iota}(\sigma) &= \sum_{0 \leq y < x < N} (-1)^y \text{sign}(\sigma(x) - \sigma(y)) \\ \hat{\hat{\iota}}(\sigma) &= \sum_{0 \leq y < x < N} (-1)^{y+x} \text{sign}(\sigma(x) - \sigma(y))\end{aligned}$$

The first statistics, $\iota(\sigma)$, is the classic and well-studied *inversion number* (e.g. [23, page 36]), up to the affine translation $\iota(\sigma) = 2\text{inv}(\sigma) - \binom{N}{2}$. The *alternating inversion number*, $\hat{\iota}(\sigma)$, was defined and studied in [5]. Along these lines, we refer to $\hat{\hat{\iota}}(\sigma)$ as the *bi-alternating inversion number* of σ .

Let $\sigma_N \in S_N$ be drawn uniformly at random. By grouping the terms according to y , one can show that each of $\iota(\sigma_N)$ and $\hat{\iota}(\sigma_N)$ follows the *Mahonian* distribution, namely

$$\frac{\iota(\sigma_N) + \binom{N}{2}}{2} = \text{inv}(\sigma_N) \sim U_1 + U_2 + \cdots + U_N$$

where each U_i is uniform in $\{0, 1, \dots, i-1\}$, and all $\{U_i\}$ are independent. By the central limit theorem, as $N \rightarrow \infty$, the normalized inversion number $3\iota(\sigma_N)/N^{3/2}$ converges in distribution to a standard Gaussian [12, page 257]. Somewhat surprisingly, Corollary 2, together with the following lemma, show that the case of $\hat{\hat{\iota}}(\sigma_N)$ is substantially different.

Lemma 4. *The following three variables follow the same distribution law.*

1. $w(\pi)$ for uniform $\pi \in S_{2n+1}$
2. $\hat{\iota}(\sigma)$ for uniform $\sigma \in S_{2n+1}$
3. $\hat{\hat{\iota}}(\sigma)$ for uniform $\sigma \in S_{2n}$

Proof. Let $\sigma \in S_{2n+1}$, and define $\tau \in S_{2n+1}$ by $\tau(x) = 2x \bmod (2n+1)$. In order to establish $w(\sigma \circ \tau) = \hat{\hat{\iota}}(\sigma)$, we compare the following sums.

$$\sum_{i=0}^{2n} \sum_{j=1}^n \text{sign}(\sigma(2(i+j)) - \sigma(2i)) = \sum_{x=1}^{2n} \sum_{y=0}^{x-1} (-1)^{y+x} \text{sign}(\sigma(x) - \sigma(y))$$

First consider x and y of equal parity. These terms correspond to $j \equiv (x-y)/2$ and $i \equiv y/2$, where all computations are in \mathbb{Z}_{2n+1} . Note that $j \in \{1, \dots, n\}$ as required. Otherwise, x and y have different parities, and we have (-1) in the term on the right. In this case, the corresponding term on the left is given by $j \equiv (y-x)/2$ and $i \equiv x/2$, and the change of sign cancels with the interchange of the minuend and the subtrahend. This proves the equivalence of (1) and (2).

Let $\rho(x) = x+1 \bmod (2n+1)$. By the symmetric definition of the writhe, it is invariant to rotations, i.e., $w(\pi \circ \rho) = w(\pi)$. Hence, so is the bi-alternating inversion number, $\hat{\hat{\iota}}(\sigma \circ \rho) = w(\sigma \circ \rho \circ \tau) = w(\sigma \circ \rho \circ \tau \circ \rho^n) = w(\sigma \circ \tau) = \hat{\hat{\iota}}(\sigma)$.

Let $\sigma \in S_{2n+1}$ be drawn uniformly. By rotation invariance, we can assume $\sigma(2n) = 2n$, without modifying the distribution of $\hat{\hat{\iota}}(\sigma)$. Consider the terms with $x = 2n$ in the definition of $\hat{\hat{\iota}}(\sigma)$. Since for these $(-1)^x = \text{sign}(\sigma(x) - \sigma(y)) = 1$, they simplify to $(-1)^y$, and their total contribution is 0. In other words, we can rotate and delete $2n$ from each permutation, and the bi-alternating inversion number is preserved. Hence (2) and (3) are equivalent as well.

It is perhaps worth remarking that the bi-alternating inversion number $\hat{\hat{\iota}}$ is no longer invariant to rotations in the even case. \square

Remark. Lemma 4 has a simple interpretation in terms of the petal diagram. The equality $w(\sigma \circ \tau) = \hat{\hat{\iota}}(\sigma)$ means that the two functions go over the $2n+1$ arcs in different orders. Instead of sorting the oriented arcs by their angles as does the writhe, $\hat{\hat{\iota}}(\sigma)$ goes over the arcs as they occur in a journey along the planar curve. For example, Figure 3A, demonstrates $w(0413265) = \hat{\hat{\iota}}(0246153) = -1$. The rotation invariance reflects the arbitrariness of choice of starting point. The transition from S_{2n+1} to S_{2n} corresponds to the act illustrated in Figure 4B.

3.2 Efficient Computation

If we take a naive approach to computing the writhe of $\pi \in S_{2n+1}$, the required time would be quadratic. It turns out that some re-arrangement can help.

Proposition 5. *Given $\pi \in S_{2n+1}$, the writhe $w(\pi)$ can be computed in time $O(n \log n)$.*

Proof. We can work with $\hat{l}(\sigma)$, where $\sigma \in S_{2n}$ is obtained from π in time $O(n)$, as described in the proof of Lemma 4.

Let $\sigma \in S_{2(l+r)}$, and denote $L = \{0, \dots, 2l-1\}$ and $R = \{2l, \dots, 2(l+r)-1\}$. We define $\sigma_L \in S_{2l}$ and $\sigma_R \in S_{2r}$, as the induced permutations on the first $2l$ and last $2r$ entries of σ , respectively. They can easily be computed via σ^{-1} in linear time.

Similar to the linking number in [11], we consider

$$lk_{LR}(\sigma) := \frac{1}{2} \sum_{y \in L} \sum_{x \in R} (-1)^{y+x} \text{sign}(\sigma(x) - \sigma(y)) = \frac{1}{2} \sum_{t=1}^{2(l+r)} y(t)(x(t) - x(t-1)),$$

where

$$x(t) := \sum_{i \in R, \sigma(i) < t} (-1)^i \quad y(t) := \sum_{i \in L, \sigma(i) < t} (-1)^i$$

The functions $x(t), y(t)$ are similarly computable via σ^{-1} in linear time, and hence so is $lk_{LR}(\sigma)$.

Finally, note that

$$\hat{l}(\sigma) = \hat{l}(\sigma_L) + \hat{l}(\sigma_R) + 2 \cdot lk_{LR}(\sigma).$$

Therefore, we can set $l = \lceil n/2 \rceil$ and $r = \lfloor n/2 \rfloor$, and proceed recursively by divide and conquer. After $\log_2 n$ divisions, we reach the base cases $\hat{l}(01) = -1$ and $\hat{l}(10) = +1$. Hence the total running time is $O(n \log n)$. \square

We remark that the above algorithm is inspired by the analogous problem on the writhe of petal diagrams. The division steps correspond to the manipulation presented in Figure 4C.

3.3 Extreme Values

How large can the writhe of a permutation $\pi \in S_{2n+1}$ get? By a direct computation, the two simple permutations $\pi(x) = x$ and $\pi(x) = 2n - x$ yield $w(\pi) = \pm n^2$. We note that these two permutations correspond to framings of the $(n+1, \pm n)$ -torus knots. The following proposition shows that these two examples are the extremes.

Proposition 6. *The writhe $w(\pi)$ of a permutation $\pi \in S_{2n+1}$ is between $\pm n^2$.*

Proof. First consider all $2n$ pairs $x, y \in \mathbb{Z}_{2n+1}$ where $\pi(x) = 0$. Clearly, each $y \in \{x+1, \dots, x+n\}$ contributes $+1$, and the other n contribute -1 each, so they cancel out. The contribution of the next $2n-1$ pairs x, y where $\pi(y) > \pi(x) = 1$ is ± 1 , depending on the distribution of such y between the two sides $\{x+1, \dots, x+n\}$ and $\{x-n, \dots, x-1\}$. Similarly, the contribution of the $2n-2$ pairs where $\pi(y) > \pi(x) = 2$ is between ± 2 , and so on. For pairs with $\pi(y) > \pi(x) \geq n$, we simply use their number as a bound.

We verify that these considerations yield the desired bound. Write

$$w(\pi) = \sum_{x=0}^{2n} w_x(\pi) \quad \text{where } w_x(\pi) := \sum_{\pi(y) > \pi(x)} \begin{cases} +1 & y \in \{x+1, \dots, x+n\} \\ -1 & y \in \{x-n, \dots, x-1\} \end{cases}$$

Then

$$|w(\pi)| \leq \sum_{x=0}^{2n} |w_x(\pi)| \leq \sum_{x=0}^{2n} \min(\pi(x), 2n - \pi(x)) = n^2$$

In fact, it follows from the argument, that equality is obtained only by the two examples mentioned above, up to rotation. \square

The symmetric group S_{2n+1} is generated by *adjacent circular transpositions* $\tau_x = (x, x+1) \in S_{2n+1}$ where $x \in \mathbb{Z}_{2n+1}$. Note that $\tau_{2n} = (2n, 0)$ is also considered an adjacent transposition. It is easy to verify that $w(\pi \circ \tau_x) - w(\pi) = \pm 2$, depending on the circular orientation of $\pi(x)$, $\pi(x+1)$ and $\pi(x+n+1)$. Consequently, the permutations $\pi(x) = x$ and $\pi(x) = 2n - x$ are at least n^2 transpositions apart from each other.

This is relevant to *circular bubble sort*. How many adjacent circular transposition are needed rearrange a circular array of N numbers in a given way? An optimal algorithm with running time $O(N^2)$ was given by Jerrum [17]. In the case of sorting the permutation $\pi(x) = x + \lfloor N/2 \rfloor$, at least $\lfloor N^2/4 \rfloor$ swaps are required due to the distance of each number from its destination. This has recently been proved to be the worst case [24]. By the above discussion, writhe considerations easily yield a very close bound of $(N-1)^2/4$ transpositions, for $\pi(x) = N - x$. This case, unlike the former, has the advantage of staying relevant in the relaxed setting of sorting up to rotations.

3.4 Circular Rank Correlation

Recall the left rotation invariance of the writhe, $w(\pi) = w(\rho^k \circ \pi)$ where $\rho(x) = x+1$ for $x \in \mathbb{Z}_{2n+1}$. Averaging $w(\rho^k \circ \pi)$ over $0 \leq k \leq 2n$ one obtains

$$w(\pi) = \sum_{0 \leq x < y \leq 2n} \alpha_n(y-x) \cdot \beta_n(\pi(y) - \pi(x))$$

where $\alpha_n, \beta_n : \mathbb{Z}_{2n+1} \setminus \{0\} \rightarrow [-1, 1]$ are

$$\alpha_n(d) := \begin{cases} +1 & d \in \{+1, \dots, +n\} \\ -1 & d \in \{-n, \dots, -1\} \end{cases} \quad \beta_n(d) := \begin{cases} +1 - \frac{2|d|}{2n+1} & d \in \{+1, \dots, +n\} \\ -1 + \frac{2|d|}{2n+1} & d \in \{-n, \dots, -1\} \end{cases}$$

In words, $\alpha_n(y-x)$ only tells from which side y is closest to x , while $\beta_n(y-x)$ is linearly dependent on their distance, giving larger weight to close pairs.

Put this way, the writhe assumes a statistical interpretation as a nonparametric statistic for circular correlation, of a certain type that we turn to describe. See [14, 21] for overview of circular data analysis.

Suppose that $(\theta_1, \phi_1), \dots, (\theta_N, \phi_N)$ are iid samples from some unknown distribution on the torus $S^1 \times S^1$. Without parametric assumptions on the distribution, we rely only on the ordering of θ_i and ϕ_i around the circle. Thus let the *circular ranks* $r_1, \dots, r_N \in \mathbb{Z}_N$ and $s_1, \dots, s_N \in \mathbb{Z}_N$ have respectively the same circular orderings as $\theta_1, \dots, \theta_N$ and ϕ_1, \dots, ϕ_N . Suppose that we want to assess how well the ϕ_i and the θ_i tend to be related by a one-to-one continuous map $S^1 \rightarrow S^1$. The case of complete dependance corresponds to $r_i = \pm s_i + k$, while if θ_i and ϕ_i are independent then $r_i = \pi(s_i)$ where $\pi \in S_N$ uniformly.

Our treatment is analogous to the case of linear rank correlation, with samples $\in \mathbb{R}^2$, where the common nonparametric statistics are Kendall's tau and Spearman's rho. A simple general form of linear correlation coefficient was given by Daniels [7]. In a similar spirit, here it is useful to consider the following general form of circular rank correlation.

$$R_{fg} = \sum_{1 \leq i < j \leq N} f\left(\frac{r_j - r_i}{N}\right) \cdot g\left(\frac{s_j - s_i}{N}\right)$$

where f and g are odd functions with period 1. Some special cases are:

1. If N is odd and the ranks are related by $s_i = \pi(r_i)$ then the writhe $w(\pi)$ is exactly $R_{\alpha\beta}$ where $\alpha(t) = \text{sign}(t)$ and $\beta(t) = \text{sign}(t)(1 - 2|t|)$ for $t \in (-\frac{1}{2}, \frac{1}{2})$.
2. Fisher and Lee's statistic Δ_N records the tendency of clockwise triples r_i, r_j, r_k to correspond to clockwise triples s_i, s_j, s_k . It is equivalent to $R_{\beta\beta}$. [13, 14]
3. An alternative measure by Fisher and Lee, following Mardia, is given by $\Pi_N = R_{\gamma\gamma}$ where $\gamma(t) = \sin(2\pi t)$. [14, 21]

Of course, the choice of statistical test depends on the assumptions on the model of association between θ_i and ϕ_i . In some applications there is no reason to assume symmetry between the two variables, e.g., due to different nature of measurement errors. In such cases, it would be interesting if an asymmetric measure such as the writhe could fit in. We are not aware of any asymmetric nonparametric statistic previously considered for circular rank correlation.

For later reference, we cite the limit theorem for Fisher and Lee's test [13]: Under the hypothesis that the two variable θ_i, ϕ_i are independent, the normalized distribution of Δ_N converges to a non-Gaussian limit distribution, given by $\frac{6}{N} R_{\beta\beta} \sim \frac{6}{\pi^2} \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \frac{1}{nm} L_{nm}$, where L_{nm} are iid Laplace random variables, with probability density $f_L(x) = \frac{1}{2} e^{-|x|}$.

4 Moments of Writhe

Here and throughout, the random variable w is the writhe of a random permutation, uniformly sampled from S_{2n+1} , or equivalently, the framing number of a random framed knot. In this section we prove Theorem 1, finding the asymptotic behavior of the moments of w . The analysis elaborates on tools used in [11] for finding the limiting moments of other knot invariants.

Remark. Recall the Gauss diagram formula of the writhe, given in Section 2. By feeding it into the computer program that we used there [11, 25], we can automatically prove $E[w^k] = O(n^k)$. This is the expected behavior of a first order invariant, cf. the main Conjecture in [11]. But here we are interested also in the constant coefficient for each k .

4.1 Never a Dull Moment

We start by deriving various expressions for the moments of w . By the reflection symmetry $w(f) = -w(-f)$, odd moments of the writhe vanish. In the following we assume k is even.

Thanks to Lemma 4, we study the distribution of the writhe via the bi-alternating inversion number.

$$E[w^k] = E_{\pi} \left[\left(\sum_{0 \leq y < x \leq 2n} (-1)^{x+y} \text{sign}(\pi(x) - \pi(y)) \right)^k \right]$$

By the linearity of the expectation,

$$E[w^k] = \sum_{\mathbf{y} < \mathbf{x}} E_{\pi} \left[\prod_{i=1}^k \text{sign}(\pi(x_i) - \pi(y_i)) \right] \cdot \prod_{i=1}^k (-1)^{x_i + y_i} \quad (1)$$

where the notation $\mathbf{y} < \mathbf{x}$ for $\mathbf{x}, \mathbf{y} \in \{0, \dots, 2n\}^k$ stands for the conjunction of $y_i < x_i$ for every $i \in \{1, \dots, k\}$. This sum needs some rearrangement.

First, we encode the ordering and the equalities between the entries of \mathbf{x} and \mathbf{y} by a directed graph, $G = (V, E)$. Both the edges and the vertices of G are labeled:

$$\begin{aligned} E(G) &= (e_1, \dots, e_k) = ((v_{11}, v_{12}), \dots, (v_{k1}, v_{k2})) \\ V(G) &= e_1 \cup \dots \cup e_k = \{1, \dots, v\} \end{aligned}$$

For each $\mathbf{x}, \mathbf{y} \in \{0, \dots, 2n\}^k$, the graph $G = G_{\mathbf{xy}}$ is defined so that the map sending y_i to v_{i1} and x_i to v_{i2} is an order preserving bijection. For example, $x_i < x_j$ iff $v_{i2} < v_{j2}$, and $x_i = y_j$ iff $v_{i2} = v_{j1}$, etc. Note that G is acyclic, with $v \leq 2k$ vertices, none of which are isolated, and possibly with parallel edges.

By the condition $\mathbf{y} < \mathbf{x}$ on each term in the sum, the vertex labeling of its graph is monotone with respect to the directed edges, i.e., $v_{i1} < v_{i2}$ for all i . We denote the collection of all such graphs by \mathcal{G}_k .

Let $G \in \mathcal{G}_k$. We define the *parity* function $\varepsilon_{\mathbf{xy}} : V(G_{\mathbf{xy}}) \rightarrow \{\pm 1\}$, such that $\varepsilon_{\mathbf{xy}}(v_{i1}) = (-1)^{y_i}$ and $\varepsilon_{\mathbf{xy}}(v_{i2}) = (-1)^{x_i}$. We also use vector notation, $\varepsilon := (\varepsilon(1), \dots, \varepsilon(v)) \in \{\pm 1\}^v$. Here and below $v := |V(G)|$.

We rewrite the above sum (1), dividing into cases according to graphs and parity.

$$E[w^k] = \sum_{G \in \mathcal{G}_k} \sum_{\varepsilon \in \{\pm\}^v} C(G, \varepsilon) A(G) T(G, \varepsilon) \quad (2)$$

where

$$C(G, \varepsilon) := \# \{ \mathbf{x}, \mathbf{y} \in \{0, \dots, 2n\}^k : G_{\mathbf{xy}} = G, \varepsilon_{\mathbf{xy}} = \varepsilon \}$$

$$T(G, \varepsilon) := \prod_{i=1}^k \varepsilon(v_{i1}) \varepsilon(v_{i2})$$

and

$$A(G) = E_\pi \left[\prod_{i=1}^k \text{sign}(\pi(x_i) - \pi(y_i)) \right]$$

for any \mathbf{x}, \mathbf{y} such that $G_{\mathbf{xy}} = G$.

Of course, we have to verify that $A(G)$ is well-defined, i.e., the right-hand side does not depend on \mathbf{x}, \mathbf{y} . Indeed, it only depends on the ordering of the $|V(G)|$ values that π assigns to the entries in \mathbf{x} and \mathbf{y} , and since π is uniform the $|V(G)|!$ orders are equally likely. In general, we define the *average sign* of a v -vertex directed graph G ,

$$A(G) := \frac{1}{v!} \sum_{\sigma \in S_v} \prod_{(i,j) \in E(G)} \text{sign}(\sigma(j) - \sigma(i))$$

To proceed with the analysis of $E[w^k]$ we borrow a definition and a lemma from [11].

Lemma 7 ([11], Lemma 11).

Let $\varepsilon \in \{\pm 1\}^v$. Denote by $z(\varepsilon)$ be the number of runs of $+$'s in ε . For example,

$$z(+++-) = 1, \quad z(+ - +) = 2$$

Equivalently,

$$z(\varepsilon_1, \dots, \varepsilon_v) = \frac{(v+1) + \varepsilon_1 - \varepsilon_1 \varepsilon_2 - \varepsilon_2 \varepsilon_3 - \dots - \varepsilon_{v-1} \varepsilon_v + \varepsilon_v}{4}$$

Then

$$\#\{0 \leq t_1 < \dots < t_v \leq 2n : \forall i \ (-1)^{t_i} = \varepsilon_i\} = \binom{n+z(\varepsilon)}{v} = \sum_{r=0}^v \binom{n}{v-r} \binom{z(\varepsilon)}{r}$$

The proof of Lemma 7 is by straightforward bijections. See [11] for more details. Now we can substitute

$$C(G, \varepsilon) = \binom{n+z(\varepsilon)}{|V(G)|}.$$

Note that $A(G)$ and $T(G, \varepsilon)$ do not depend on the underlying parameter n . Hence (2) expresses $E[w^k]$ as a polynomial in n , computable in finite time for each k . For example, for $k = 2, 4$ we evaluate all terms and obtain the following.

Proposition 8. Let w be the writhe of $\pi \in S_{2n+1}$, sampled uniformly at random. Then

$$E[w^2] = \frac{2n^2 + n}{3} \quad E[w^4] = \frac{76n^4 + 44n^3 - 49n^2 - 26n}{45}$$

The treatment of the leading term of the k th moment is similar to [11], with partitions or patterns replaced by graphs. Recall that the functions $\chi(I)(\varepsilon_1, \dots, \varepsilon_v) = \prod_{i \in I} \varepsilon_i$, where $I \subseteq \{1, \dots, v\}$, constitute an orthogonal basis of the 2^v -dimensional space of functions $\{\pm 1\}^v \rightarrow \mathbb{R}$, and $\langle \chi(I), \chi(J) \rangle = \sum_{\varepsilon} \chi(I)(\varepsilon) \chi(J)(\varepsilon) = 2^v \delta_{IJ}$. The *degree* of a function $f : \{\pm 1\}^v \rightarrow \mathbb{R}$ is defined as

the largest $|I|$ in its representation, $f = \sum_I \phi_I \chi(I)$, where $\phi_I \neq 0$. By Lemma 7, $\deg z = 2$ as a function of $\varepsilon \in \{\pm 1\}^v$. For $r \leq v/2$, one can verify that $\deg \binom{z}{r} = 2r$. In these terms, (2) becomes

$$E[w^k] = \sum_{G \in \mathcal{G}_k} A(G) \langle C(G, \varepsilon), T(G, \varepsilon) \rangle = \sum_{G \in \mathcal{G}_k} A(G) \sum_{r=0}^v \binom{n}{v-r} \left\langle \binom{z}{r}, \chi(I_G) \right\rangle \quad (3)$$

where I_G is the set of vertices in G with odd total degree. Note that $|I_G|$ is even, and $|I_G| \geq 2(v-k)$ with equality iff all vertices have total degree 1 or 2. The terms $\binom{n}{v-r} \langle \binom{z}{r}, \chi(I_G) \rangle$ divide into cases:

- If $r > v - k$ then $\binom{n}{v-r} = O(n^{k-1})$.
- If $r < v - k$ then $\langle \binom{z}{r}, \chi(I_G) \rangle = 0$, since $\deg \binom{z}{r} = 2r < 2v - 2k \leq |I_G|$.
- If $r = v - k < |I_G|/2$ then similarly the term vanishes by orthogonality.
- If $r = v - k = |I_G|/2$, we have $\binom{n}{k} \langle \binom{z}{|I_G|/2}, \chi(I_G) \rangle$.

Note that this means $E[w^k] = O(n^k)$.

We characterize the graphs that make nonzero contribution to the sum in (3). Which components in the expansion of $\binom{z}{r}$ according to the basis $\{\chi(I)\}_I$ have degree $2r$? By examining the expression for $z(\varepsilon)$ in Lemma 7, every I that is a union of r disjoint pairs of consecutive numbers appears in $\binom{z}{r}$ with coefficient $(-\frac{1}{4})^r$. Denote by \mathcal{G}_k^* the graphs in \mathcal{G}_k , with I_G of this form and maximal total degree 2. Every v -vertex graph in \mathcal{G}_k^* contributes $\binom{n}{k} (-\frac{1}{4})^r 2^v = \binom{n}{k} (-1)^v 2^{2k-v}$.

Example. Let $G = (\text{graph with 9 vertices and 6 edges}) \in \mathcal{G}_6^*$, where the $v = 9$ vertices are labeled by $\{1, \dots, 9\}$ from left to right, and the $k = 6$ edge are labeled arbitrarily. Then $I_G = \{2, 3, 6, 7, 8, 9\}$, which is composed of $r = 3$ consecutive pairs. Its contribution to $E[w^6]$ is equal to $-2^3 \binom{n}{6}$.

Dividing (3) by n^k , and neglecting lower order terms, we write the limiting moments of the normalized writhes as

$$\mu_k := \lim_{n \rightarrow \infty} E \left[\left(\frac{w(\pi_{2n+1})}{n} \right)^k \right] = \frac{1}{k!} \sum_{G \in \mathcal{G}_k^*} (-1)^{v(G)} 2^{2k-v(G)} A(G) \quad (4)$$

Let \mathcal{G}_k^2 be the 2-regular graphs in \mathcal{G}_k . Each $G \in \mathcal{G}_k^*$ is obtained from *breaking* some $G' \in \mathcal{G}_k^2$, defined as splitting some subset of the degree-two vertices into pairs of degree-one vertices, while preserving the order of the vertex labels. We denote breaking by $G \prec G'$.

Example. We break 3 vertices of the graph $G' = (\text{graph with 9 vertices and 6 edges}) \in \mathcal{G}_6^2$ to obtain G from the previous example. A different labeled graph for the same breaking is $(\text{graph with 9 vertices and 6 edges})$.

Note that there are 2^k ways to break a k -vertex graph at a subset of its vertices, and each breaking of r vertices corresponds to 2^r labeled graphs in \mathcal{G}_k^* , as each pair of resulting degree-one vertices can be ordered in 2 ways. Therefore, (4) becomes

$$\mu_k = \frac{2^k}{k!} \sum_{G' \in \mathcal{G}_k^2} B(G') \quad B(G') := \sum_{G \prec G'} (-1)^{v(G)} A(G) \quad (5)$$

The sum on the right is only over the 2^k ways to break G' . Instead of caring for the 2^{v-k} different vertex labelings of the same breaking, we have multiplied each breaking by 2^{v-k} .

Let $\sigma \in S_k$. We define a 2-regular directed graph G_σ , with vertices $\{1, \dots, k\}$ and edges $\{i, \sigma(i)\}$ which are always directed from the smaller number to the larger one. We replace the summation over $G' \in \mathcal{G}_k^2$ in (5) by summation over $\sigma \in S_k$.

$$\mu_k = \sum_{\sigma \in S_k} 2^{k-|\text{cycles}(\sigma)|} B(G_\sigma) \quad (6)$$

Indeed, we multiplied by $k!$ since each G_σ corresponds to $k!$ edge labelings of $G' \in \mathcal{G}_k^2$. We then divided by 2 once for every cycle of σ , since both orientations of a cycle in σ yield the same cycle in G_σ . Note that G_σ may contain parallel edges in case of cycles of length 2, in which case we divide by 2 as well, but for another reason – we have half the number of edge labelings for G_σ .

4.2 Euler Numbers and Eulerian Numbers

We suspend for a while our efforts to rewrite μ_k , for the sake of finding $A(G)$ and $B(G')$. To that end, we'll use some classical notions in Enumerative Combinatorics. An *alternating* permutation $\pi \in S_m$, is defined by the condition $\pi(1) < \pi(2) > \pi(3) < \pi(4) > \dots \pi(m)$. The number of alternating permutations in S_m , here denoted by A_m , is called the *Euler number* [23]. Their exponential generating functions was given by André as follows.

$$\begin{aligned} \sec x &= 1 + \frac{1}{2!}x^2 + \frac{5}{4!}x^4 + \frac{61}{6!}x^6 + \dots + \frac{A_m}{m!}x^m + \dots & m \text{ even} \\ \tan x &= \frac{1}{1!}x + \frac{2}{3!}x^3 + \frac{16}{5!}x^5 + \frac{272}{7!}x^7 + \dots + \frac{A_m}{m!}x^m + \dots & m \text{ odd} \end{aligned}$$

A *descent* in a permutation $\pi \in S_m$ is a pair $\pi(i) > \pi(i+1)$ where $i \in \{1, \dots, m-1\}$. The number of permutation in S_m with d descents is the *Eulerian number* $A_{m,d}$. The following relation between the Euler numbers and the Eulerian numbers goes back to Euler [10, 23].

$$\sum_{d=0}^{m-1} (-1)^d A_{m,d} = \begin{cases} (-1)^{(m-1)/2} A_m & \text{if } m \text{ is odd} \\ 0 & \text{if } m \text{ is even} \end{cases}$$

Finally, the odd Euler numbers are related to the *Bernoulli numbers*, via

$$B_m = (-1)^{m/2+1} \frac{m}{2^m(2^m-1)} A_{m-1} \quad \text{for even } m \geq 2$$

Let P_m be an oriented path with m edges, and let C_m be a cyclically oriented circle with m edges. The following lemma gives the average sign of oriented paths and cycles.

Lemma 9. *Let $A(G)$ be as in (2).*

$$A(P_{m-1}) = -A(C_{m+1}) = \begin{cases} \frac{(-1)^{(m-1)/2}}{m!} A_m & \text{if } m \text{ is odd} \\ 0 & \text{if } m \text{ is even} \end{cases}$$

Examples. $A(\bullet \rightarrow \bullet) = -1$, $A(\bullet \rightarrow \bullet \rightarrow \bullet) = -A(\bullet \rightarrow \bullet \rightarrow \bullet) = \frac{1}{3}$, $A(\bullet \rightarrow \bullet \rightarrow \bullet \rightarrow \bullet) = \frac{2}{15}$.

Proof. The edges of P_{m-1} are $(i, i+1)$ for $i \in \{1, \dots, m-1\}$. The product $\prod_i \text{sign}(\sigma(i+1) - \sigma(i))$ is exactly $(-1)^d$ where d is the number of descents in σ . Hence the average over σ is the alternating sum $\frac{1}{m!} \sum_d (-1)^d A_{m,d}$, and we use the above identity for the Eulerian numbers.

In the cycle C_{m+1} , consider the vertex $i = \sigma^{-1}(m+1)$ given $\sigma \in S_{m+1}$. Note that the product $\text{sign}(\sigma(i) - \sigma(i-1)) \cdot \text{sign}(\sigma(i+1) - \sigma(i))$ equals $(+1) \cdot (-1)$ regardless of the rest of σ . The remaining m vertices constitute a path P_{m-1} on which σ is uniform in S_m , as before. Hence $A(C_{m+1}) = -A(P_{m-1})$. \square

By the next set of observations, knowing the average sign $A(G)$ for oriented paths and cycles is all we need to evaluate (5).

Lemma 10. *Let $A(G)$ be the average sign of G as before.*

1. If G_1 is obtained from G_2 by flipping the direction of one edge, then $A(G_1) = -A(G_2)$.
2. If the number of edges in G is odd, then $A(G) = 0$.
3. If G is the disjoint union of connected components G_1, \dots, G_l then $A(G) = \prod_i A(G_i)$.

Proof. All parts are fairly straightforward from the definition:

1. Note that $\text{sign}(\sigma(i) - \sigma(j))$ changes for exactly one edge.
2. Equivalently summing over $\bar{\sigma}(i) := \sigma(v+1-i)$ yields a factor of $(-1)^{\#\text{edges}}$.
3. The restriction of $\sigma \in S_m$ to each connected component is independently uniform. \square

We turn to compute $B(G')$, the alternating sum of $A(G)$ over all the breakings $G \prec G'$, where G' is a disjoint union of cycles. Note that the above-mentioned three properties naturally carry over from A to B . Hence it suffices to know B for an even oriented cycle.

Lemma 11. *For $m \geq 2$,*

$$B(C_m) = \frac{-2^m B_m}{m!}$$

Proof. Each proper breaking of C_m is an ordered partition of the cycle into r oriented paths, of lengths $m_1 + \dots + m_r = m$. By Lemmas 10,

$$B(C_m) = A(C_m) + \sum_{r=1}^m (-1)^r \frac{m}{r} \sum_{m_1 + \dots + m_r = m} A(P_{m_1}) A(P_{m_2}) \dots A(P_{m_r})$$

Indeed, we multiplied by m since we can start the breaking at any vertex in C_m , and divided by r to avoid over-counting, since any of the r parts could serve as the starting point.

We write a generating function.

$$\sum_{m=1}^{\infty} B(C_m) x^m = \sum_{m=1}^{\infty} A(C_m) x^m + \sum_{m=1}^{\infty} m x^m \sum_{r=1}^m \frac{(-1)^r}{r} \sum_{\Sigma m_i = m} A(P_{m_1}) \dots A(P_{m_r})$$

Lemma 9 yields generating functions for $A(C_m)$ and $A(P_m)$:

$$\tanh x = \sum_{m \text{ odd}} \frac{(-1)^{(m-1)/2} A_m x^m}{m!} = - \sum_{m=1}^{\infty} A(C_m) x^{m-1} = x + \sum_{m=1}^{\infty} A(P_m) x^{m+1}$$

A sequence of standard manipulations on power series yields:

$$-x \frac{d}{dx} \log \left(1 + \sum_{m=1}^{\infty} c_m x^m \right) = \sum_{m=1}^{\infty} m x^m \sum_{r=1}^m \frac{(-1)^r}{r} \sum_{\Sigma m_i = m} c_{m_1} c_{m_2} \dots c_{m_r}$$

We substitute the above, and obtain:

$$\sum_{m=1}^{\infty} B(C_m) x^m = -x \tanh x - x \frac{d}{dx} \log \left(1 + \frac{\tanh x - x}{x} \right) = 1 - x \coth x$$

This yields the desired result via another expansion [16, p. 42]: $x \coth x = 1 + \sum_{m=2}^{\infty} 2^m B_m x^m / m!$ \square

We now proceed from oriented cycles to any union of cycles. An *excedance* in a permutation $\sigma \in S_k$ is a pair $i < \sigma(i)$, while a pair $i > \sigma(i)$ is called a *deficiency*. The number of deficiencies is denoted by $\text{def}(\sigma)$.

Lemma 12. *Let $\sigma \in S_k$, and let G_σ be as defined for (6).*

$$B(G_\sigma) = \prod_{\gamma \in \text{cycles}(\sigma)} (-1)^{\text{def}(\gamma)} B(C_{|\gamma|})$$

Proof. B is multiplicative at the different cycles by Lemma 10. The cyclic graph corresponding to $\gamma \in \text{cycles}(\sigma)$ is turned into $C_{|\gamma|}$ by flipping $\text{def}(\gamma)$ edges, corresponding to deficiencies. \square

The cycles structure of a permutation $\sigma \in S_m$ induces a partition $X_1 \cup \dots \cup X_r = [m]$. Given a set X_i , denote by $Z(X_i)$ the collection of $(|X_i| - 1)!$ cycles composed of these elements. The following lemma provides the average parity of deficiencies in a cycle.

Lemma 13.

$$\frac{1}{|Z(X)|} \sum_{\gamma \in Z(X)} (-1)^{\text{def}(\gamma)} = A(C_{|X|})$$

Proof. By considering the cyclic notation $(1, \sigma(1), \sigma^2(1), \dots)$, one obtains equivalence between the distribution of descents in all permutations, and deficiencies in cyclic permutations. In particular, the sum of $(-1)^{\text{def}(\sigma)}$ over cyclic $\sigma \in S_m$, is given by $\pm A_{m-1}$, just as in Lemma 9. \square

We finally return to (6) and simplify the limiting moments. By Lemmas 12-13

$$\begin{aligned} \frac{\mu_k}{2^k} &= \sum_{\sigma \in S_k} \frac{B(G_\sigma)}{2^{|\text{cycles}(\sigma)|}} = \sum_{X_1, \dots, X_r} \prod_{i=1}^r \sum_{\gamma \in Z(X_i)} \frac{(-1)^{\text{def}(\gamma)} B(C_{|\gamma|})}{2} = \\ &= \sum_{X_1, \dots, X_r} \prod_{i=1}^r |Z(X_i)| \cdot \frac{A(C_{|X_i|}) B(C_{|X_i|})}{2} = \sum_{\sigma \in S_k} \prod_{\gamma \in \text{cycles}(\sigma)} \frac{A(C_{|\gamma|}) B(C_{|\gamma|})}{2} \end{aligned}$$

Substituting A and B from Lemmas 9,11 proves Theorem 1.

5 Limit Distribution

We prove Corollary 2, showing that the distribution of the normalized writhe, $W_{2n+1} = w(\pi)/n$ where $\pi \in S_{2n+1}$ uniformly, weakly converges to a limit W . We then study some representations and properties of the limit distribution.

5.1 Proof of Corollary 2

Partition the sum over permutations in Theorem 1, according to the cycle lengths.

$$\mu_k = \sum_{\sigma \in S_k} \prod_{\gamma \in \text{cycles}(\sigma)} \lambda_{|\gamma|} = \sum_{r=1}^{\infty} \frac{1}{r!} \sum_{m_1 + \dots + m_r = k} \frac{k!}{m_1 m_2 \dots m_r} \lambda_{m_1} \lambda_{m_2} \dots \lambda_{m_r}$$

Indeed, every *ordered* set of r cycles that constitute σ will be counted $r!$ times, hence the factor $(1/r!)$. If the cycle lengths are m_1, \dots, m_r , then the number of assignments of numbers $\{1, \dots, k\}$ to the elements of all cycles is $k!/m_1 m_2 \dots m_r$, because of equivalence to rotation of each cycle. Thus the moment generating function is

$$\mathcal{M}(z) = \sum_{k=0}^{\infty} \frac{\mu_k}{k!} z^k = 1 + \sum_{r=1}^{\infty} \frac{1}{r!} \prod_{j=1}^r \sum_{m_j=1}^{\infty} \frac{\lambda_{m_j}}{m_j} z^{m_j} = \exp \left(\sum_{m=1}^{\infty} \frac{\lambda_m}{m} z^m \right)$$

Since asymptotically $|B_m| \sim 2 \cdot m!/(2\pi)^m$ for even $m \rightarrow \infty$, we have [16, p. 1041]

$$\lambda_m = \frac{8^m (2^m - 1) B_m^2}{2(m!)^2} \sim 2 \left(\frac{2}{\pi} \right)^{2m}$$

Hence $\log \mathcal{M}(z)$ has radius of convergence $\pi^2/4$. This implies:

1. The moment generating function $\mathcal{M}(z)$ is analytic at $z = 0$.
2. A limit distribution W exists, uniquely defined by its moments $E[W^k] = \mu_k$ (e.g. [4, 9]).
3. The tails of W decay at exponential asymptotic rate, $\frac{1}{t} \log P[|W| > t] \xrightarrow{t \rightarrow \infty} -\pi^2/4$. \square

5.2 Integral Representation

Consider the characteristic function of W :

$$\varphi_W(t) = \exp \left(\sum_{m=2}^{\infty} \frac{8^m (2^m - 1) B_m^2}{2m(m!)^2} (it)^m \right)$$

It turns out that the infinite series can be replaced with an integral. By the expansions [16, p. 42]

$$t \cot 2t = \sum_{m=0}^{\infty} \frac{(4i)^m B_m}{2 \cdot m!} t^m \quad \log \cosh t = \int_0^t \tanh u du = \sum_{m=2}^{\infty} \frac{2^m (2^m - 1) B_m}{m!} \cdot \frac{t^m}{m}$$

we represent the characteristic function as a Hadamard product,

$$\varphi_W(t) = \exp(t \cot 2t \circ \log \cosh t) \quad \text{where} \quad \left(\sum a_n t^n \right) \circ \left(\sum b_n t^n \right) = \left(\sum a_n b_n t^n \right)$$

which equals the integral

$$(f \circ g)(t) = \int_0^1 f(e^{2\pi i u}) g(te^{-2\pi i u}) du = \frac{1}{2\pi i} \oint_{|z|=1} f(z) g\left(\frac{t}{z}\right) \frac{dz}{z}$$

Therefore, the characteristic function of W is given by the contour integral

$$\varphi_W(t) = \exp\left(\frac{1}{2\pi i} \oint_{|z|=1} \cot(2z) \log \cosh(t/z) dz\right)$$

5.3 Series Representations

We study the characteristic function of W by another approach. Recall that the Bernoulli numbers appear as certain values for the Riemann zeta function. For even $m \geq 2$,

$$\zeta(m) = \sum_{n=1}^{\infty} \left(\frac{1}{n}\right)^m = -\frac{(2\pi i)^m B_m}{2 \cdot m!}$$

Hence $\varphi_W(t) =$

$$\exp\left(-\sum_{m=2}^{\infty} \frac{4^m (2^m - 1) B_m t^m}{m \cdot m! \cdot \pi^m} \sum_{n=1}^{\infty} \left(\frac{1}{n}\right)^m\right) = \exp\left(-\sum_{n=1}^{\infty} \sum_{m=2}^{\infty} \frac{2^m (2^m - 1) B_m}{m \cdot m!} \left(\frac{2t}{\pi n}\right)^m\right)$$

By the above-mentioned expansion of $\log \cosh$,

$$\varphi_W(t) = \exp\left(-\sum_{n=1}^{\infty} \log \cosh\left(\frac{2t}{\pi n}\right)\right) = \prod_{n=1}^{\infty} \operatorname{sech}\left(\frac{2t}{\pi n}\right) = \prod_{n=1}^{\infty} \varphi_A\left(\frac{t}{n}\right)$$

where A is a random variable with characteristic function $\varphi_A(t) = \operatorname{sech}(2t/\pi)$, and density function $f_A(x) = \frac{1}{\pi} \operatorname{sech} x$. By Lévy's Continuity Theorem,

$$W \sim \sum_{n=1}^{\infty} \frac{A_n}{n} \quad \text{where } A_n \sim A \text{ iid}$$

It follows that W has a continuous density function, and it is also infinitely divisible (see [19]). Repeating this manipulation on A yields [16, p. 45]

$$\varphi_A(t) = \operatorname{sech}\left(\frac{2t}{\pi}\right) = \prod_{k=1}^{\infty} \left(1 + \frac{16t^2}{(2k-1)^2 \pi^4}\right)^{-1} = \prod_{k=1}^{\infty} \varphi_L\left(\frac{4t}{(2k-1)\pi^2}\right)$$

where $\varphi_L(t) = 1/(1+t^2)$ is the characteristic function of the Laplace distribution, with probability density function $f_L(x) = \frac{1}{2} e^{-|x|}$. Equivalent definitions are $L \sim (E_1 - E_2) \sim (Z_1 Z_2 + Z_3 Z_4)$ where E_i and Z_i are respectively iid exponential and iid normal variables. In conclusion,

$$W \sim \frac{4}{\pi^2} \sum_{n=1}^{\infty} \sum_{\substack{m=1 \\ \text{odd}}}^{\infty} \frac{L_{mn}}{mn} \quad \text{where } L_{mn} \sim L \text{ iid}$$

5.4 Remark

Note the similarity between the limit of the writhe and that of Fisher and Lee's statistic Δ_N from Section 3.4. The summation of $\frac{1}{mn}L_{mn}$, there over $m, n \in \mathbb{N}$, is here restricted to odd m . Further investigation of this comparison suggests a limit theorem for circular rank correlation, which we sketch below.

Recall the general form R_{fg} for circular rank correlation, from Section 3.4. For both the writhe and Δ_N , the normalized limit distribution is given by $\frac{1}{4} \sum_{m,n} \lambda_m \kappa_n L_{mn}$, where λ_m and κ_n are the respective Fourier coefficients of f and g , i.e., $f(t) = \sum_m \lambda_m \sin(2\pi mt)$ and $g(t) = \sum_n \kappa_n \sin(2\pi nt)$. From the theory of U -statistics, we know that this is indeed the case for the *parametric* statistic

$$U_{fg} = \sum_{i < j} f(\theta_j - \theta_i) g(\phi_j - \phi_i)$$

under the hypothesis that all θ_i and ϕ_i are iid uniform in $[0, 1]$. The joint distribution of the normalized ranks $\frac{1}{N}r_i$ and $\frac{1}{N}s_i$ that appear in R_{fg} instead, is more complicated. However, some condition on f and g would ensure that $\frac{1}{N}(R_{fg} - U_{fg}) \rightarrow 0$ in probability, and hence equality of the limit laws.

References

- [1] C. Adams, T. Crawford, B. DeMeo, M. Landry, A. T. Lin, M. Montee, S. Park, S. Venkatesh, and F. Yhee. Knot projections with a single multi-crossing. *Journal of Knot Theory and Its Ramifications*, 24(03), 2015.
- [2] C. C. Adams. *The knot book*. American Mathematical Soc., 1994.
- [3] A. Borodin, P. Diaconis, and J. Fulman. On adding a list of numbers (and other one-dependent determinantal processes). *Bulletin of the American Mathematical Society*, 47(4):639–670, 2010.
- [4] L. Breiman. *Probability, volume 7 of Classics in Applied Mathematics*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992.
- [5] D. Chebikin. Variations on descents and inversions in permutations. *Electron. J. Combin.*, 15(1):R132, 2008.
- [6] S. Chmutov, S. Duzhin, and J. Mostovoy. *Introduction to Vassiliev knot invariants*. Cambridge University Press, 2012.
- [7] H. E. Daniels. The relation between measures of correlation in the universe of sample permutations. *Biometrika*, pages 129–135, 1944.
- [8] P. Diaconis and A. Ram. Analysis of systematic scan metropolis algorithms using Iwahori-Hecke algebra techniques. *The Michigan Mathematical Journal*, 48(1):157–190, 2000.
- [9] R. Durrett. *Probability: theory and examples*. Cambridge university press, 2010.
- [10] L. Euler. Remarques sur un beau rapport entre les séries des puissances tant directes que réciproques. *E352 (Eneström Index)*, 1768.
- [11] C. Even-Zohar, J. Hass, N. Linial, and T. Nowik. Invariants of random knots and links. *arxiv.org:1411.3308*, submitted for publication, 2014.
- [12] W. Feller. *An introduction to probability theory and its applications*, volume 1. John Wiley & Sons, 1968.
- [13] N. Fisher and A. Lee. Nonparametric measures of angular-angular association. *Biometrika*, 69(2):315–321, 1982.
- [14] N. I. Fisher. *Statistical analysis of circular data*. Cambridge University Press, 1995.
- [15] C. F. Gauss. General theory of terrestrial magnetism. *Taylor's Scientific Memoirs*, 2:184–251, 1841.
- [16] I. Gradshteyn, A. Jeffrey, I. Ryzhik, and D. Zwillinger. *Table of integrals, series, and products*. Academic Press, 2007.
- [17] M. R. Jerrum. The complexity of finding minimum-length generator sequences. *Theoretical Computer Science*, 36:265–289, 1985.
- [18] L. H. Kauffman. *On knots*. Number 115 in Annals of Mathematics Studies. Princeton University Press, 1987.
- [19] P. Lévy. Wiener's random function, and other Laplacian random functions. In *Second Berkeley Symposium on Mathematical Statistics and Probability*, volume 1, pages 171–187, 1951.
- [20] C. L. Mallows. Non-null ranking models. i. *Biometrika*, pages 114–130, 1957.
- [21] K. V. Mardia. Statistics of directional data. *Journal of the Royal Statistical Society. Series B (Methodological)*, pages 349–393, 1975.
- [22] J. A. Mingo and A. Nica. On the distribution of the area enclosed by a random walk on \mathbb{Z}^2 . *Journal of Combinatorial Theory, Series A*, 84(1):55–86, 1998.
- [23] R. P. Stanley. *Enumerative combinatorics*. Cambridge University Press, 1999.
- [24] A. van Zuylen, J. Bieron, F. Schalekamp, and G. Yu. An upper bound on the number of circular transpositions to sort a permutation. *arXiv preprint arXiv:1402.4867*, 2014.
- [25] Ancillary files at <http://arxiv.org/abs/1411.3308>, 2014.